

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

THE UNITED STATES OF AMERICA,

Plaintiff,

-against-

ROMAN STORM, ET AL.,

Defendant.

Case No. 23 Cr. 430 (KPF)

Oral Argument: July 12, 2024

DEFENDANT ROMAN STORM'S
REPLY IN SUPPORT OF MOTION TO SUPPRESS

Brian E. Klein
Keri Curtis Axel
Kevin M. Casey
Waymaker LLP
515 S. Flower Street, Suite 3500
Los Angeles, California 90071
(424) 652-7800

Attorneys for Roman Storm

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	ARGUMENT	2
A.	The Government Lacks Any Justification for the Indiscriminate Seizure of “Any and All Cryptocurrency”	2
B.	The Government’s Concession That the Subject Cryptocurrency Is Not Physically Located in Roman Storm’s Home or on His Devices Fatally Undermines the Premises Search Warrant	4
C.	The Search Warrant Cannot Be Used to Seize Assets for Forfeiture Purposes	8
III.	CONCLUSION	12

TABLE OF AUTHORITIES

Cases

<i>Kaley v. United States</i> , 571 U.S. 320 (2014).....	10
<i>Matter of Search of One Address in Washington, D.C. Under Rule 41 (“One Address”)</i> , 512 F. Supp. 3d 23 (D.D.C. 2021).....	3, 4
<i>United States v. \$16,072.00 in U.S. Currency</i> , 374 F. Supp. 3d 205 (N.D.N.Y. 2019).....	9
<i>United States v. 113 Virtual Currency Accts.</i> , No. CV 20-606 (TJK), 2024 WL 940141 (D.D.C. Mar. 5, 2024).....	7
<i>United States v. 155 Virtual Currency Assets</i> , No. 20-CV-2228 (RC), 2021 WL 1340971, at *6 (D.D.C. Apr. 9, 2021).....	7
<i>United States v. 50.44 Bitcoins</i> , No. CV ELH-15-3692, 2016 WL 3049166 (D. Md. May 31, 2016).....	7
<i>United States v. All Assets Held at Bank Julius Baer & Co., Ltd.</i> , 571 F. Supp. 2d 1 (D.D.C. 2008).....	6
<i>United States v. Aventura Technologies, Inc.</i> , 607 F. Supp. 3d 278 (E.D.N.Y. 2022)	7
<i>United States v. Axelson</i> , No. 17 Cr. 0225 (PJS/HB), 2018 WL 614476 (D. Minn. Jan. 9, 2018).....	11
<i>United States v. Bikundi</i> , 125 F. Supp. 3d 178 (D.D.C. 2015).....	10
<i>United States v. Field</i> , 62 F.3d 246 (8th Cir. 1995)	9
<i>United States v. Fisher</i> , 225 F. Supp. 3d 151 (W.D.N.Y. 2016).....	10
<i>United States v. Galpin</i> , 720 F.3d 436 (2d Cir. 2013).....	3
<i>United States v. Gotti</i> , 155 F.3d 144 (2d Cir. 1998).....	9

<i>United States v. Kwok</i> , No. 23 CR. 118 (AT), 2024 WL 989806 (S.D.N.Y. Mar. 7, 2024)	7
<i>United States v. Perkins</i> , 994 F. Supp. 2d 272 (E.D.N.Y. 2014)	9
<i>United States v. Queri</i> , 679 F.Supp.2d 295 (N.D.N.Y. 2010)	10
<i>United States v. Ripinsky</i> , 20 F.3d 359 (9th Cir. 1994)	9
<i>United States v. Weigand</i> , 482 F. Supp. 3d 224, 242–43 (S.D.N.Y. 2020), as corrected (Sept. 2, 2020).....	6
<i>Zurcher v. Stanford Daily</i> , 436 U.S. 547 (1978).....	6
Statutes	
18 U.S.C. § 1963(d)(1)(A)	9
18 U.S.C. § 981	6
21 U.S.C. § 853	2, 6, 8, 9, 10
Other Authorities	
U.S. Dep’t of Just., Asset Forfeiture Policy Manual § 3.D (2023)	8
Rules	
Federal Rule of Criminal Procedure 41(b)(6)(A)	passim

I. INTRODUCTION

The government's opposition brief only further supports what Roman Storm proved in his suppression motion: that, to the extent it purported to authorize the seizure of property not within the curtilage of his home, the premises search warrant exceeded the bounds of the Fourth Amendment and settled procedural safeguards governing search and seizure warrants.

The government effectively admits that the warrant was both overbroad and lacking in particularity. To wit, its statement that Mr. Storm's cryptocurrency "may" constitute fruits of a crime is a concession that the government still does not have probable cause to believe that "any and all cryptocurrency" is evidence. That evidence "may" be found among an individual's property is constitutionally insufficient to allow the government to rummage through such property.

As to the fact that the warrant purports to permit the seizure of material that is not within the curtilage of the home, the government has no meaningful response. While admitting that cryptocurrency does not in fact reside on unhosted wallets, which are just a species of an electronic device, the government resorts to fearmongering straw man arguments, proposing that protecting Mr. Storm's Fourth Amendment rights would impede the government's examination of lawfully-seized electronic devices and prevent seizure of cryptocurrency. Neither of these propositions is true, or reflects Mr. Storm's position. The government also misdirects to an inapposite venue provision in Federal Rule of Criminal Procedure 41(b)(6)(A), which does not provide it authority to search locations that are beyond the scope of the search warrant.

Finally, the government suggests that the Court can simply treat this search warrant as a forfeiture seizure warrant, but that is simply not what it is. If the government wants to seize assets in anticipation of forfeiture, it needs to follow the proper procedure and seek a seizure

warrant, supported by probable cause and meeting the statutory requirements of 21 U.S.C. § 853(f) and settled case law interpreting it. The government has not done so and, on the current record, such a warrant would not be justified based on the absence of probable cause reflected in the search warrant and its opposition.

Just as the government could not seize all of a defendant's bank accounts without a seizure warrant that satisfied the Fourth Amendment and the well-established standards for pre-forfeiture seizure of assets, the government should not be permitted to use Mr. Storm's private keys to rifle around the blockchain to seize "any and all" of what it believes is Mr. Storm's cryptocurrency and transfer that cryptocurrency to its own wallets. The Court should reject this wholesale assault on the Fourth Amendment.

II. ARGUMENT

A. The Government Lacks Any Justification for the Indiscriminate Seizure of "Any and All Cryptocurrency"

Without any logical or factual support, the government claims that the warrant provides sufficient probable cause for the seizure of "any and all cryptocurrency" (Dkt. 53, Gov't Opposition ("Opp.") at 95-97), but its opposition admits otherwise. The government simply recites the affidavit's allegations that \$2.6 million of cryptocurrency was transferred to unhosted wallets owned by Mr. Storm following the imposition of OFAC sanctions. (*See* Dkt. 27-1, Ex. A at ¶¶ 5(g), 12.) From there, the government jumps to the conclusion that "[a]ccordingly, there is probable cause to conclude that any and all cryptocurrency found at and seized from the defendant's residence may constitute the fruits of the Subject Offenses and therefore was well within the bounds of the Warrant." (Opp. at 95-96.)

The government's assertion is a non-sequitur. The transfer of some cryptocurrency under circumstances the government finds suspicious does not provide probable cause to believe that

“any and all cryptocurrency” is somehow contraband subject to seizure. Indeed, the government’s own language—that the cryptocurrency “may” constitute the fruits of the alleged offenses—demonstrates the fallacy in its argument. Any money or thing of value *may* constitute the fruits of criminal activity, but that alone does not constitute probable cause.

The government goes on to admit that it “is not yet in a position to determine which, if any, cryptocurrency that the [g]overnment may eventually access pursuant to the [w]arrant constitutes the fruits of the [s]ubject [o]ffenses.” (Opp. at 96.) This is a stunning admission that the government does not currently have (and obviously did not have at the time of the warrant’s issuance) probable cause to believe that “any and all cryptocurrency” is subject to seizure. Instead, the government is simply on a fishing expedition to see if it can find evidence of a crime. This is exactly the sort of “general, exploratory rummaging in a person’s belongings” that the Fourth Amendment does not allow. *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013).

The case cited by the government, *Matter of Search of One Address in Washington, D.C. Under Rule 41* (“*One Address*”), 512 F. Supp. 3d 23, 30 (D.D.C. 2021), does not support its argument. First, and most obviously, as a magistrate judge’s decision in the District of Columbia, *One Address* is not binding on this Court and indeed carries no more weight than the Tacoma magistrate judge’s decision to issue the warrant in this case. Second, the warrant in *One Address*, while referencing Rule 41, was in fact a seizure warrant seeking forfeitable property which, as explained in Mr. Storm’s motion to suppress and below, is different from the search warrant at issue. (See Dkt. 27, Mot. to Suppress at 12.) Accordingly, the magistrate made findings under the forfeiture statute that are not present here. Third, the basis for the broad seizure of “all cryptocurrency” in *One Address* was that it was being used to facilitate the crime

of possession of child pornography. 512 F. Supp. 3d at 25. Here, there is no claim that Mr. Storm was using his cryptocurrency to commit the alleged offenses.

Allowing for the seizure of “any and all cryptocurrency” accessed via the seized wallets is very much akin to allowing agents to seize a bank card and then using that card to empty the subject’s bank accounts. (See Dkt. 27-3, Perklin Aff. at ¶ 8 (“Private keys are analogous to client cards issued by modern banks (*i.e.*, bank cards).”).) The government attempts to fight this analogy,¹ but its protests just make the point more clear. The only distinction the government can draw is that they cannot as easily issue subpoenas for cryptocurrency as they can for bank records. (See Opp. at 97.) But the government’s investigative challenges do not constitute probable cause.² The fact remains that the government has failed to establish probable cause to believe that “any and all cryptocurrency” it might find after using the seized wallets is evidence or fruits of a crime.

B. The Government’s Concession That the Subject Cryptocurrency Is Not Physically Located in Roman Storm’s Home or on His Devices Fatally Undermines the Premises Search Warrant

The government acknowledges, as it must, that cryptocurrency is not located in Mr. Storm’s home or even on the devices it seized but “*exists entirely on the Internet.*” (Opp. at 98 (emphasis added); see also *id.* citing Perklin Aff. at ¶ 7 (“[u]nits of cryptocurrency reside on their associated blockchain”); and *id.* (“cryptocurrency itself only exists in digital form on the

¹ Notably, the government takes no issue with the facts in Mr. Perklin’s declaration; nor could it.

² This claim also fails on the facts. The government does not need a subpoena for cryptocurrency in the same way it does for fiat currency, because cryptocurrency is traceable on the blockchain. As the magistrate judge wrote in *One Address*, with cryptocurrency, “every transaction is publicly documented from cradle to grave on the blockchain. 512 F. Supp. 3d at 30 n.11. Accordingly, “cryptocurrency—be it in hosted or unhosted wallets—is traceable and seizable.” *Id.* at 30. The fact is that, using the information on a subject’s lawfully-seized devices, an agent can easily trace assets connected with the keys on that device and does not need a subpoena to do so.

Internet.”)³ However, the government claims that agents are nevertheless authorized to use the devices to access the cryptocurrency that is admittedly located on a blockchain elsewhere, relying on Rule 41(b)(6)(A). (*See Opp.* at 98.)

Rule 41(b)(6)(A) is a venue provision and does not create substantive authority to conduct searches beyond the scope of a search warrant. Rule 41(b) is titled “Venue for a Warrant Application” and provides the boundaries within which a magistrate judge may issue a warrant. Mr. Storm is not challenging that his home was within the magistrate judge’s district and that venue was therefore proper, at least as to items within the curtilage of the home. Subsection (b)(6)(A) provides for a different scenario, namely that a magistrate judge may “issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if ...the district where the media or information is located has been concealed through technological means.” But that is not the type of warrant that was issued here. The warrant instead makes clear that the property to be searched consisted of Mr. Storm’s home and the items to be seized included the electronic devices “found therein.” (Dkt. 27-1, Ex. A at Attachment A.) Nothing in Rule 41(b)(6)(A) gives agents authority to go beyond the express terms of the search warrant.

Nor could any rule of criminal procedure grant such authority. The requirement that searches be limited to the property that is the subject of a warrant derives from the Fourth

³ Given these concessions to fact, it’s a bit surprising to see the government blithely continuing to parrot the counter-factual proposition that cryptocurrency existed “in the residence,” when it well knows it did not. (*See Opp.* at 99 (“cryptocurrency ‘found in the defendant’s residence’”); *id.* (warrant reaches “any cryptocurrency found in the defendant’s residence”); *id.* at 100 (“cryptocurrency in the residence”).) The government is all too willing to make unsupported and flat-out-wrong claims as to cryptocurrency; these claims are presented to magistrates in search warrants every day and, as here, warrants are issued based on false factual premises that fail Constitutional and procedural standards.

Amendment. *See, e.g., Zurcher v. Stanford Daily*, 436 U.S. 547, 556 (1978). Rule 41 is meant to reflect Fourth Amendment protections, not constrict them. *See id.* at 558. In short, the Federal Rules of Criminal Procedure do not and cannot trump the Constitution.

Because it has no credible legal basis to seize items that it admits were not within the premises to be searched, the government instead misdirects, attempting to produce fear through “straw man” arguments that Mr. Storm did not raise. First, the government suggests that Mr. Storm seeks to undermine its ability to access and search the electronic devices (including wallets) that it seized. (*See Opp.* at 98.) This is untrue: Mr. Storm has not challenged the government’s probable cause showing to access his electronic devices, including the private key information on those devices. The issue is that the government cannot—without a properly issued seizure warrant under 21 U.S.C. § 853 or 18 U.S.C. § 981—use those passcodes to go out on the internet and seize any of Mr. Storm’s cryptocurrency, much less “any and all” of it. *See e.g., United States v. Weigand*, 482 F. Supp. 3d 224, 242–43 (S.D.N.Y. 2020), as corrected (Sept. 2, 2020) (“Of course, the warrant did not authorize the [g]overnment to search other locations ... or to use passwords that it found. Rather, if the [g]overnment uncovered evidence showing that further evidence of the conspiracy existed in other locations, it would then need to seek another warrant.”).

Second, the government suggests that accepting Mr. Storm’s argument would place cryptocurrency in unhosted wallets “beyond the reach of US law enforcement.” (*Id.*) This also misstates Mr. Storm’s argument and raises a false fear. The government knows how to obtain authority to seize bank account proceeds—assets that, like cryptocurrency, do not physically reside in a subject’s home or at the bank. *See, e.g., United States v. All Assets Held at Bank Julius Baer & Co., Ltd.*, 571 F. Supp. 2d 1 (D.D.C. 2008) (civil forfeiture action for assets held

by bank); *United States v. Kwok*, No. 23 CR. 118 (AT), 2024 WL 989806, at *1 (S.D.N.Y. Mar. 7, 2024) (discussing bank accounts seized by the government after “obtaining the requisite warrants”); *United States v. Aventura Technologies, Inc.*, 607 F. Supp. 3d 278, 281 (E.D.N.Y. 2022) (discussing authorized seizure warrant for bank accounts containing property traceable to the charged criminality). The government also knows how to obtain authority to seize and forfeit cryptocurrency. *See, e.g., United States v. Firoz Patel*, No. 23-CR-166 (DLF), 2024 WL 1932871, at *4 (D.D.C. May 1, 2024) (“[T]he government performed its blockchain-tracing analysis... before the seizure of the 450 bitcoin... It was this very tracing evidence that led to the seizure of the 450 bitcoin[.]”).⁴ Should the government follow this well-trodden path to obtain a seizure warrant for cryptocurrency, upon probable cause and with appropriate tracing (as further explained below), there is no issue that it has authority to do so. But it did not follow those steps here.

Rather, here, the government used false factual claims in the agent’s affidavit—suggesting that cryptocurrency is “on” a wallet when it well knows it is not—to obtain a search warrant under Rule 41, seeking an end run around the established limits of the Fourth Amendment and the forfeiture statutes. Because the warrant seeks to seize cryptocurrency that

⁴ *See also United States v. 155 Virtual Currency Assets*, No. 20-CV-2228 (RC), 2021 WL 1340971, at *6 (D.D.C. Apr. 9, 2021) (“The [g]overnment further alleges that, through blockchain analysis, it identified the accounts used in the scheme as the [d]efendant [p]roperties. The [g]overnment has provided documented trails of bitcoin transfers originating from several named organizations.”); *United States v. 113 Virtual Currency Accts.*, No. CV 20-606 (TJK), 2024 WL 940141, at *5 (D.D.C. Mar. 5, 2024) (forfeiture complaint described “property with reasonable particularity, given that it identifie[d] the 145 cryptocurrency account addresses and detail[ed] the complex series of transactions at issue); *United States v. 50.44 Bitcoins*, No. CV ELH-15-3692, 2016 WL 3049166, at *2 (D. Md. May 31, 2016) (after subject voluntarily transferred 50.44 bitcoins to agents, they obtained a seizure warrant for bitcoins and initiated forfeiture proceedings).

was not within the curtilage of Mr. Storm's home, this Court should find that the warrant is simply unconstitutional.

C. The Search Warrant Cannot Be Used to Seize Assets for Forfeiture Purposes

The government incorrectly claims that because the search warrant references both “search” and “seizure”, it can seize “any and all cryptocurrency” for some possible future forfeiture proceeding pursuant to a premises search warrant. (Opp. at 99.) Tellingly, the government finds Mr. Storm's argument “mystifying,” but that is because it clearly does not appreciate the differences between a search warrant pursuant to Rule 41 and a warrant for the pre-forfeiture seizure of assets under 21 U.S.C. § 853(f). As a Rule 41 search warrant, the warrant to search Mr. Storm's home could only authorize the search and seizure of evidence of a crime, contraband, fruits of crime, or items illegally possessed or used in committing a crime. The government is wrong to claim that Rule 41 seizure is a “lawful precursor to secure assets so that they may be later forfeited upon conviction.” (Opp. at 99.) Rather, seizure under Rule 41 serves the purposes of finding and preserving evidence; once the evidence “loses its evidentiary value”⁵ (or if it never has it in the first place), the government “must obtain a seizure warrant or restraining order to maintain custody of the property for forfeiture.” *See* U.S. Dep't of Just., Asset Forfeiture Policy Manual § 3.D at pp. 2-8 (2023); *see also United States v. \$16,072.00 in*

⁵ While Mr. Storm does not concede that any of his devices has ever had evidentiary value, he has not challenged the seizure of any device (whether phone, computer, or wallet) under Rule 41. Accordingly, contrary to the government's claim (Opp. at 99), Mr. Storm's position is not inconsistent with respect to the types of devices seized. The issue is that the government seeks to seize assets not on the premises to be searched which, on these facts, only affects the wallet devices. Had the warrant purported to provide the government authority to use the banking app on his phone to go out and transfer money from his bank account to a government account, however, Mr. Storm would have challenged that as beyond the scope of a Rule 41 premises warrant, as he has challenged the warrant's constitutionally-violative authorization to sweep “any and all” of his cryptocurrency.

U.S. Currency, 374 F. Supp. 3d 205, 210 (N.D.N.Y. 2019) (“[I]f the government’s continued possession of property is based only on its evidentiary value, the government must seek an alternative basis to maintain possession if and when that evidentiary value evaporates.”).

To seize property for the purpose of pre-forfeiture seizure of assets, the government is required to obtain a seizure warrant pursuant to 21 U.S.C. § 853(f), which provides:

The [g]overnment may request the issuance of a warrant authorizing the seizure of property subject to forfeiture under this section in the same manner as provided for a search warrant. If the court determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that an order under subsection (e) may not be sufficient to assure the availability of the property for forfeiture, the court shall issue a warrant authorizing the seizure of such property.

Like Rule 41, subsection (e) of section 853 permits a restraining order or bond to be issued only to restrain property associated with the crime. 21 U.S.C. § 853(a)(1) (authorizing seizure of “any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation”); *see United States v. Gotti*, 155 F.3d 144, 150 (2d Cir. 1998) (interpreting parallel provision of 18 U.S.C. § 1963(d)(1)(A) to reject pretrial restraint of substitute assets due to “unambiguous language” of the statute); *United States v. Perkins*, 994 F. Supp. 2d 272, 276 (E.D.N.Y. 2014) (applying *Gotti* to Section 853 as provisions are “substantially identical” and ordering government to release property seized as a substitute asset; *see also United States v. Field*, 62 F.3d 246, 249 (8th Cir. 1995) (substitute assets not subject to pretrial restraint); *United States v. Ripinsky*, 20 F.3d 359, 365 (9th Cir. 1994) (same)). Accordingly, even if the government had sought (or were to seek) a pre-forfeiture seizure warrant (which it has not), it could not seize “any and all” of Mr. Storm’s cryptocurrency that could be accessed through the seized devices because substitute assets cannot be restrained pre-trial.

Similarly, under the statute and Supreme Court precedent, for a seizure order to be constitutionally permissible, “[t]here must be probable cause to think (1) that the defendant has committed an offense permitting forfeiture, and (2) that the property at issue has the requisite connection to that crime.” *Kaley v. United States*, 571 U.S. 320, 323-24 (2014). Simply put, if assets are not traceable to the alleged crime, they are not seizable pre-trial. *See, e.g., United States v. Bikundi*, 125 F. Supp. 3d 178, 195 (D.D.C. 2015) (ordering assets released where the affidavits failed to show a requisite connection to the offenses); *United States v. Fisher*, 225 F. Supp. 3d 151, 172 (W.D.N.Y. 2016) (citing *United States v. Queri*, 679 F.Supp.2d 295, 296 (N.D.N.Y. 2010)) (“In contrast to directly forfeitable property and its traceable proceeds, the [g]overnment ‘may not obtain a pre-trial restraint on potential substitute property.’”). Here, the government made no effort—in the affidavit in support of the search warrant or in its opposition—to establish that “any and all” cryptocurrency on Mr. Storm’s wallet had a connection to the crime, and indeed it could never do so.

The government did not obtain a seizure warrant or invoke 21 U.S.C. § 853(f) in seeking the seizure of Mr. Storm’s property. Nor could the search warrant be so construed. Notably, the search warrant fails to establish probable cause that “any and all cryptocurrency” even constitutes evidence or fruits of a crime, much less that it “would, in the event of conviction, be subject to forfeiture.” 21 U.S.C. § 853(f). And the search warrant utterly fails to explain why an order pursuant to subsection (e) would not be sufficient to assure the availability of the property for forfeiture. The government has not sought an order pursuant to subsection (e), nor could it because the government cannot show that “any and all cryptocurrency” “has the requisite connection to [the alleged] crime.” *Kaley*, 571 U.S. at 324.

The lone district case relied upon by the government has nothing to do with the distinction between search warrants and forfeiture warrants. (*See Opp.* at 100, citing *United States v. Axelson*, No. 17 Cr. 0225 (PJS/HB), 2018 WL 614476, at *7 (D. Minn. Jan. 9, 2018), *report and recommendation adopted*, No. 17 Cr. 0225 (PJS/HB), 2018 WL 614735 (D. Minn. Jan. 29, 2018).) In *Axelson*, the district court addressed the defendant’s argument that permitting the seizure of the defendant’s computers and electronic devices did not permit the search of those items. It said nothing about using the contents of seized devices to go out on the internet and seize other property. As explained above, Mr. Storm does not here challenge the government’s showing to seize and search electronic devices on his premises, only the legality of seizing “any and all cryptocurrency” that can be accessed by using the keys on such devices. Accordingly, *Axelson* is wholly inapplicable.

Mr. Storm does not challenge the search or seizure of his electronic devices,⁶ but only the wholesale seizure of “any and all cryptocurrency” that may be found by accessing the information on those devices. Such a seizure cannot be justified procedurally, legally, or constitutionally, under the search warrant issued in this case.

//

//

//

//

//

⁶ To be clear, Mr. Storm does not challenge the seizure and search of his electronic devices based on any deficiencies in the warrant application, such as Fourth Amendment challenges including a lack of probable cause, but of course reserves rights to raise any challenge that might later become apparent such as (1) a search continuing for an indefinite period of time or (2) continued seizure of the devices beyond the point of their evidentiary value.

III. CONCLUSION

For all the reasons above and in the motion to suppress, the Court should grant suppression.

Dated: May 24, 2024

Respectfully submitted,

/s/ Brian E. Klein

Brian E. Klein
Keri Curtis Axel
Kevin M. Casey
Waymaker LLP

Attorneys for Roman Storm